CertShared now are offering 100% pass ensure 70-744 dumps!
https://www.certshared.com/exam/70-744/ (216 Q&As)

Microsoft
Exam Questions 70-744
Securing Windows Server 2016
NEW QUESTION 1
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.


The relevant objects in the domain are configured as shown in the following table.

<table>
<thead>
<tr>
<th>Server name</th>
<th>Object</th>
<th>Organizational unit (OU) name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server1</td>
<td>Computer account</td>
<td>Servers</td>
</tr>
<tr>
<td>Server2</td>
<td>Computer account</td>
<td>Servers</td>
</tr>
<tr>
<td>User1</td>
<td>User account</td>
<td>Operations Users</td>
</tr>
</tbody>
</table>

You need to assign User1 the right to restore files and folders on Server1 and Server2. Solution: You add User1 to the Backup Operators group in contoso.com.

Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation: References:

The solution would let User1 to backup files and folders on domain controllers for contoso.com instead.

NEW QUESTION 2

You create a new bastion forest named admin.contoso.com. The forest functional level of admin.contoso.com is Windows Server 2012 R2.

You need to implement a Privileged Access Management (PAM) solution.

Which two actions should you perform? Each correct answer presents part of the solution.

A. Raise the forest functional level of admn.contoso.com.
B. Deploy Microsoft Identity Management (MIM) 2016 to admin.contoso.com.
C. Configure contoso.com to trust admin.contoso.com.
D. Deploy Microsoft Identity Management (MIM) 2016 to contoso.com.
E. Raise the forest functional level of contoso.com.
F. Configure admin.contoso.com to trust contoso.com.

Answer: DE


For the bastion forest which deploys MIM, you should raise the Forest Functional Level to “Windows Server 2016”?

NEW QUESTION 3

The domain contains a server named Server1 that has Microsoft Security Compliance Manager (SCM) 4.0 installed.

You export the baseline shown in the following exhibit.
You have a server named Server2 that is a member of a workgroup. You copy the \(2617e9b1-9672-492b-aefa-0505054848c2\) folder to Server2. You need to deploy the baseline settings to Server2. What should you do?

A. Download, install, and then run the Lgpo.exe command.
B. From Group Policy Management import a Group Policy object (GPO).
C. From Windows PowerShell, run the Restore-GPO cmdlet.
D. From Windows PowerShell, run the Import-GPO cmdlet.
E. From a command prompt run the sededit.exe command and specify the /import parameter.

Answer: D

Explanation: References: https://anytecho.wordpress.com/2015/05/22/importing-group-policies-using-powershell-almost/

NEW QUESTION 4

Your network contains an Active Directory domain named contoso.com. You install the Windows Server Update Services server role on a member server named Server1. Server1 runs Windows Server 2016. You need to ensure that a user named User1 can perform the following tasks:
* View the Windows Server Update Services (WSUS) configuration.
* Generate WSUS update reports.

The solution must use the principle of least privilege. What should you do on Server1?

A. Modify the permissions of the ReportWebService virtual folder from the WSUS Administration website.
B. Add User1 to the WSUS Reporters local group.
C. Add User1 to the WSUS Administrators local group.
D. Run vsussutil.exe and specify the postinstall parameter.

Answer: B

Explanation: WSUS Reporters have read only access to the WSUS database and configuration.
When a user with “WSUS Reporters” membership, he can view configuration and generate reports as follow:

NEW QUESTION 5
Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.
A central access policy named Policy1 is deployed to the domain. You need to apply Policy1 to Volume1.
Which tool should you use?

A. File Explorer  
B. Shared Folders  
C. Server Manager  
D. Disk Management  
E. Storage Explorer  
F. Computer Management  
G. System Configuration  
H. File Server Resource Manager (FSRM)

**Answer:** A

**Explanation:**
“File Explorer” = “Windows Explorer”.
https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/deploy-a-central-access-policy--demonstration-steps--#BKMK_1.4

**NEW QUESTION 6**

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. You have an organizational unit (OU) named Administration that contains the computer account of Server1. You import the Active Directory module to Server1. You create a Group Policy object (GPO) named GPO1. You link GPO1 to the Administration OU. You need to log an event each time an Active Directory cmdlet is executed successfully from Server1. What should you do?

A. From Advanced Audit Policy in GPO1 configure auditing for directory service changes.  
B. Run the `(Get-Module ActiveDirectory).LogPipelineExecutionDetails - $false` command.  
C. Run the `(Get-Module ActiveDirectory).LogPipelineExecutionDetails = $true` command.  
D. From Advanced Audit Policy in GPO1 configure auditing for other privilege use event

**Answer:** C

**NEW QUESTION 7**

Your network contains an Active Directory domain named contoso.com. The domain contains multiple servers that run multiple applications. Domain user accounts are used to authenticate access requests to the servers. You plan to prevent NTLM from being used to authenticate to the servers. You start to audit NTLM authentication events for the domain. You need to view all of the NTLM authentication events and to identify which applications authenticate by using NTLM. On which computers should you review the event logs and which logs should you review?

A. Computers on which to review the event logs: Only client computers  
B. Computers on which to review the event logs: Only domain controllers  
C. Computers on which to review the event logs: Only member servers  
D. Event logs to review: Applications and Services Logs\Microsoft\Windows\Diagnostics- Networking\Operational  
E. Event logs to review: Applications and Services Logs\Microsoft\Windows\NTLM\Operational  
F. Event logs to review: Applications and Services Logs\Microsoft\Windows\SMBClient\Security  
G. Event logs to review: Windows Logs\Security  
H. Event logs to review: Windows Logs\System

**Answer:** AE

**Explanation:** Do not confuse this with event ID 4776 recorded on domain controller’s security event log!!!
This question asks for implementing NTLM auditing when domain clients is connecting to member servers! See below for further information.
Via lab testing, most of the NTLM audit logs are created on Windows 10 clients, except that you use Windows Server 2016 OS as clients (but this is unusual)
NEW QUESTION 8
HOTSPOT
Your network contains an Active Directory domain named contoso.com. You plan to deploy an application named App1.exe. You need to verify whether Control Flow Guard is enabled for App1.exe. Which command should you run? To answer, select the appropriate options in the answer area.

Answer:

Control Flow Guard (CFG) is a highly-optimized platform security feature that was created to combat memory corruption vulnerabilities.
By placing tight restrictions on where an application can execute code from, it makes it much harder for exploits to execute arbitrary code through vulnerabilities such as buffer overflows.

To verify if Control Flow Guard is enabled for a certain application executable:- Run the dumpbin.exe tool (included in the Visual Studio 2015 installation) from the Visual Studio command prompt with the /headers and /loadconfig options: dumpbin.exe /headers /loadconfig test.exe.
The output for a binary under CFG should show that the header values include "Guard", and that the load config values include "CF Instrumented" and "FID table present".1
NEW QUESTION 9
You have a server named Server1 that runs Windows Server 2016. You configure Just Enough Administration (JEAD) on Server1.

You need to view a list of commands that will be available to a user named User1 when User1 establishes a JEA session to Server1. Which cmdlet should you use?

A. Trace-Command
B. Get-PSSessionCapability
C. Get-PSSessionConfiguration
D. Show-Command

Answer: B

The `Get-PSSessionCapability` cmdlet gets the capabilities of a specific user on a constrained session configuration. Use this cmdlet to audit customized session configurations for users. Starting in Windows PowerShell 5.0, you can use the RoleDefinitions property in a session configuration (.pssc) file. Using this property lets you grant users different capabilities on a single constrained endpoint based on group membership. The `Get-PSSessionCapability` cmdlet reduces complexity when auditing these endpoints by letting you determine the exact capabilities granted to a user. This command is used by IT Administrator (The “You” mention in the question) to verify configuration for a User.

NEW QUESTION 10
You enable and configure PowerShell Script Block Logging.

You need to view which script blocks were executed by using Windows PowerShell scripts. What should you do?

A. View the Microsoft-Windows-Powershell/Operational event log.
B. Open the log files in %LocalAppData%\Microsoft\Windows\PowerShell.
C. View the Windows PowerShell event log.
D. Open the log files in %SYSTEMROOT%\Log

Answer: A

Explanation: [Link](https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit_script)
After you enable detailed script tracing, Windows PowerShell logs all script blocks to the event log, MicrosoftWindows-Powershell/Operational.
NEW QUESTION 11
You have a server named Server1 that runs Windows Server 2016.
You need to identify the default action for the inbound traffic when Server1 connects to the domain. Which cmdlet should you use?

A. Get-NetIPSecRule
B. Get-NetFirewallRule
C. Get-NetFirewallProfile
D. Get-NetFirewallSetting
E. Get-NetFirewallPortFilter
F. Get-NetFirewallAddressFilter
G. Get-NetFirewallApplicationFilter

Answer: C

NEW QUESTION 12
You have the Windows Server 2016 operating system images as following table.

<table>
<thead>
<tr>
<th>Image name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image1</td>
<td>A Nano Server that runs the Standard edition of Windows Server</td>
</tr>
<tr>
<td>Image2</td>
<td>A Server Core installation that runs the Datacenter edition of Windows Server</td>
</tr>
<tr>
<td>Image3</td>
<td>A Full installation that runs the Standard edition of Windows Server</td>
</tr>
<tr>
<td>Image4</td>
<td>A Nano Server that runs the Datacenter edition of Windows Server</td>
</tr>
</tbody>
</table>

Your company’s security policy states that you must minimize the attack surface when provisioning new servers.
You need to deploy a Host Guardian Service cluster. Which image should you use for the deployment?

A. image1
B. image2
C. image3
D. image4

Answer: C


Prerequisites
Hardware: HGS can be run on physical or virtual machines, but physical machines are recommended. If you want to run HGS as a three-node physical cluster (for availability), you must have three physical servers.
(As a best practice for clustering, the three servers should have very similar hardware.)
Server Roles: Host Guardian Service and supporting server roles.
Configuration permissions/privileges for the fabric (host) domain: You will need to configure DNS forwarding between the fabric (host) domain and the HGS domain.
If you are using Admin-trusted attestation (AD mode), you will need to configure an Active Directory trust between the fabric domain and the HGS domain.
NEW QUESTION 13
Solution: From a Group Policy, you configure the Security Options. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 14
You need to ensure that when users access files in shared folders on the network, the files are encrypted when they are transferred over the network.
Solution: You enable access-based enumeration on all the file shares. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation: Access-Based Enumeration does not help encrypting network file transfer.

NEW QUESTION 15
DRAG DROP
Which three cmdlets should you run in sequence? To answer move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.
NEW QUESTION 16
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows10. The network uses the 172.16.0.0/16 address space.
Computer1 has an application named App1.exe that is located in D:\Apps\. App1.exe is configured to accept connections on TCP port 8080. You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.
Solution: You run the New-NetFirewallRule –DisplayName "Rule1" –Direction Inbound –Program "D:\Apps\App1.exe" –Action Allow -Profile Domain command. Does this meet the goal?
A. Yes
B. No

Answer: A

NEW QUESTION 17
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. A user named User1 is a member of the local Administrators group.
Server1 has the AppLocker rules configured as shown in the exhibit. (Click the Exhibit button.) Exhibit:

![AppLocker configuration](image)

Rule1 and Rule2 are configured as shown in the following table.

<table>
<thead>
<tr>
<th>Rule name</th>
<th>Path</th>
<th>File hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule1</td>
<td>D: \Folder1 * *</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Rule2</td>
<td>Not applicable</td>
<td>App2.exe</td>
</tr>
</tbody>
</table>

You verify that User1 is unable to run App2.exe on Server1.
Which changes will allow User1 to run D:\Folder1\Program.exe and D:\Folder2\App2.exe? To answer select the appropriate options in the answer area.

**Answer:**

**Explanation:** References:

**NEW QUESTION 18**

**HOTSPOT**
You plan to implement a guarded fabric in TPM-trusted attestation mode. The fabric will contain a three-node Host Guardian Service (HGS) cluster and four guarded hosts. All the hosts will have matching hardware and will run the same workload. You need to add the hosts to the HGS cluster.
What is the minimum number of times you must run each cmdlet to implement the HGS cluster? To answer, select the appropriate options in the answer area.
**NOTE:** Each correct selection is worth one point.
Certshared now are offering 100% pass ensure 70-744 dumps!
https://www.certshared.com/exam/70-744/ (216 Q&As)

Answer:

Explanation:

References:

NEW QUESTION 19

......
Thank You for Trying Our Product

**We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions
2nd - Questions and Answers in PDF Format

**70-744 Practice Exam Features:**

* 70-744 Questions and Answers Updated Frequently
* 70-744 Practice Questions Verified by Expert Senior Certified Staff
* 70-744 Most Realistic Questions that Guarantee you a Pass on Your First Try
* 70-744 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click 
Order The 70-744 Practice Test Here